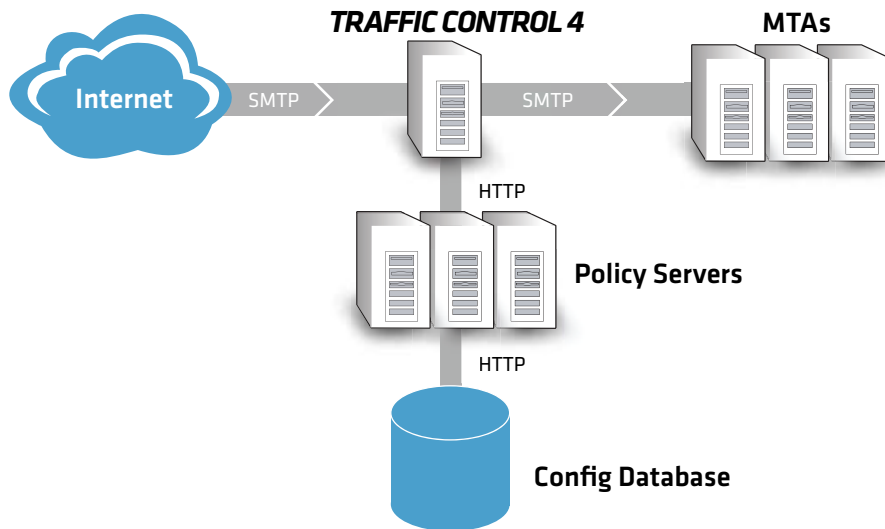


BRIEFING: POLICY DELEGATION



Traffic Control™ 4 provides a flexible extension mechanism which allows for the delegation of message handling policy to a cluster of separate policy servers. The policy delegation mechanism works as follows:

1. Traffic Control sends a brief summary of the connection state to the cluster of policy servers. Connection state can be sent at any phase of the SMTP session (CONNECT, HELO, MAIL, RCPT, DATA, etc). Connection state includes everything that Traffic Control knows about the connection, such as the results of any configured RBL lookups, the client's host name and IP address, and any recipients specified so far.
2. The policy server contacts a configuration database and determines what should be done with the SMTP session, responding to Traffic Control with a set of actions. Actions include altering the recipient list, rejecting the connection with a defined error message, making log entries in Traffic Control's log, etc. Traffic Control supports arbitrary configuration of policy server clusters with hot-failover and load balancing.
3. Once Traffic Control receives the policy server's response, it takes the specified actions on the SMTP session.

The policy delegation protocol is a simple text-based protocol that rides on top of the Hypertext Transfer Protocol (HTTP). Using HTTP allows implementation of the policy server software using off-the-shelf web server technologies such as Java™ Servlets and the Common Gateway Interface (CGI). A reference implementation of the policy server is available.

REQUEST MESSAGE FORMAT

- Protocol names are ESMTP or SMTP.
- Protocol states are CONNECT, EHLO, HELO, MAIL, RCPT, DATA, END-OF-MESSAGE, VRFY or ETRN; these are the SMTP protocol states where the Traffic Control SMTP server makes an OK/REJECT/HOLD/ etc. decision.
- The “request” attribute is required. In this example the request type is “smtpd_access_policy”.
- The “recipient” attribute is available in the “RCPT TO” stage. It is also available in the “DATA” and “END-OF-MESSAGE” stages if Traffic Control accepted only one recipient for the current message.
- The “recipient_count” attribute is non-zero only in the “DATA” and “END-OF-MESSAGE” stages. It specifies the number of recipients that Traffic Control accepted for the current message.
- The client address is an IPv4 dotted quad in the form 1.2.3.4 or it is an IPv6 address in the form 1:2:3::4:5:6.
- The client name is the verified, double reversed lookup, of the client IP address. This attribute will not be present if the A record for the reverse PTR lookup does not match the client IP address or is non-existent.
- The reverse_client_name is the name found from a PTR lookup on the client IP address.
- The “transaction_id” attribute value can be used to correlate different requests regarding the same message delivery.
- The “size” attribute value specifies the message size that the client specified in the MAIL FROM command (zero if none was specified). It specifies the actual message size when the client sends the END-OF-DATA command.
- The “encryption_*” attributes specify information about how the connection is encrypted. With plaintext connections the protocol and cipher attributes are empty and the keysize is zero.
- The “rbl_check” attribute specifies an rbl_zone and the IPv4 dotted quad result the following format: <rbl_zone>:<result>.
- The “cloudmark_score” attribute specifies the message score on a scale from 0 to 100 as determined by the Cloudmark filtering system.
- The “cloudmark_category” attribute specifies the type of message as determined by the Cloudmark filtering system. Currently the only defined category is “virus”.

EXAMPLE REQUEST

Traffic Control sends the SMTP session state document to the Policy Service via an HTTP POST request. The following is an example of how such a request might look on the wire:

```
POST /trex/policy_service HTTP/1.1
Content-Length: 1234

request=smtpd_access_policy
protocol_state=RCPT
protocol_name=SMTP
helo_name=some.domain.tld
transaction_id=8045F2AB23
sender=foo@bar.tld
recipient=bar@foo.tld
recipient_count=0
client_address=1.2.3.4
client_name=another.domain.tld
reverse_client_name=another.domain.tld
size=12345
encryption_protocol=TLSv1/SSLv3
encryption_cipher=DHE-RSA-AES256-SHA
encryption_keysize=256
rbl_check=zen.spamhaus.org:127.0.0.1
cloudmark_score=100
[empty line]
```

NOTES

- The order of the attributes does not matter. The policy server should ignore any attributes that it does not care about.
- When the same attribute name is sent more than once, the server may keep the first value or the last attribute value.
- When an attribute value is unavailable, the client either does not send the attribute, sends the attribute with an empty value ("name="), or sends a zero value ("name=0") in the case of a numerical attribute.
- An attribute name must not contain "=", null or newline, and an attribute value must not contain null or newline.

RESPONSE MESSAGE FORMAT

- The “action” attribute is the only response attribute.

RESPONSE ACTIONS

- **OK** – Allow the session to continue without applying anymore policy restrictions.
- **4NN text** – Defer this stage of the session by responding with the numerical three digit code and text. The reply code “421” causes Traffic Control to disconnect immediately after sending the response.
- **5NN text** – Reject this stage of the session by responding with the numerical three digit code and text.
- **REJECT optional text** – Reject this sage of the session by responding with the default reject code for the stage and optional text when specified, otherwise reply with a generic error message.
- **DEFER optional text** – Defer this sage of the session by responding with the default defer code for the stage and optional text when specified, otherwise reply with a generic error message.
- **BCC user@domain** – Send one copy of the message to the specified recipient.
- **DISCARD optional text** – Claim successful delivery and silently discard the message. Log the optional text if specified, otherwise log a generic message.
- **ADD_HEADER headername: headervalue** – Prepend the specified message header to the message.
- **REDIRECT user@domain** – Send the message to the specified address instead of the intended recipients.
- **WARN optional text** – Log a warning with the optional text, together with client information and if available, with helo, sender, recipient and protocol information.

EXAMPLE RESPONSE

```
200 OK
Content-Length: 1234

action=BCC user@domain
action=ADD_HEADER X-Spam-Verdict: OK
action=WARN This policy was delegate
[empty line]
```



» 602 W. Hastings St, Suite 601
Vancouver, BC V6B 1P2

www.mailchannels.com
info@mailchannels.com

toll-free +1 888 685 7488
main +1 604 685 7488
fax +1 604 608 9490